

REMARKS

OA states rejected claims 1, 4-8, 10-15, and 18-20 under 35 U.S.C. 103(a) as being unpatentable over Kocher et al. U. S. Patent No. 6,304,658 (Kocher), and claims 2, 3, 9, 16 and 17 as being unpatentable over Kocher et al. U. S. Patent No. 6,304,658 in view of Kawan et al. U. S. Patent No. 7,039,812 (Kawan). Before turning to specific limitations of specific claims, for clarity's sake, applicant briefly summarizes the teachings, and contrasts the present disclosure (PD) with the cited prior art documents.

The PD teaches an optimal "door opening" strategy, balancing the needs of security with practicality. Public key encryption is very secure, but computationally intensive, while shared key encoding is less secure but more expedient. The PD does not claim new ground in either public key, or shared key, cryptography. The invention is in the optimized use of both. The PD also has inventive ways to integrate biometric identification into this scheme. In contrast, Kocher teaches breaking new security grounds in public key cryptography, and Kawan teaches conventional biometric security. Applicant respectfully avers that these two documents do not render obvious the scope of the claims in the PD.

Regarding Kocher's teachings, in detail: The important point in this regard is that the PD teaches the use of full blown public key encoding, (apart of initial set up) only during rare randomly chosen challenges. This approach lead to both security and simplicity. Kocher says nothing of combining public key and shared key approach, and, particularly, has nothing on random challenges. Applicant would respectfully suggest that the OA misunderstood Kocher on this point. In reference to claim 15 of the PD, which explicitly states a "challenge is issued on randomly selected occasions" the OA cites Kocher col. 5, lines 51 - 59. Here Kocher says: "Typically the server sends a unique, unpredictable challenge value R to the user's token, which computes the value $A=H(R||K)$, where "||" denotes concatenation and H is a one-way cryptographic hash function such as SHA. The user sends A to the server, which independently computes A (using its copy of K) and compares its result with the received value. The user authentication succeeds only if the comparison operation indicates a match." - - -

The randomness referred to in this section by Kocher is the "unpredictable challenge value R", that is the value of R is what is random, (as of course it should be, otherwise it would not serve as a secret) and not the occasion of the challenge. Careful reading of all of Kocher's

specification also come up empty regarding random challenges. The PD has the challenge itself, box 230 in Fig. 2, as a random occurrence. Kocher has no hint, or suggestion along these lines, accordingly, applicant would respectfully point out that Kocher does not render obvious the claims (some amended) of the PD.

Applicant amended claim 1 and claim 10, for both explicitly adding the limitation of the random nature of the challenge. For claim 10, this meant including the limitation of claim 15, and canceling claim 15. Independent claim 4 already has the random selection limitation included, and applicant suggests that it is patentable over Kocher without amending. Applicant further submits that if independent claims 1, 4, and 10 are patentable, then all non-canceled dependent claims, by introducing further limitations, are a fortiori patentable.

However, there are limitations in some dependent claims that have to be noted, since these by themselves are novel, and not taught in the art. Claims 6 and 12 recognize that in some cases, as detailed in the specification of the PD, for instance, page 4 lines 11 - 16, communication can even be sent without encryption and still not jeopardize the overall security of the scheme, while, again, speeding up the transactions. OA citation of Kocher col. 5, lines 51 - 55 re claims 6 and 12, was already quoted above. And, to the contrary of the OA assertion, Kocher teaching says that what the server, which is the door in the PD, does is to encode the random "R".

Regarding biometrics and the teaching by Kawan: The fundamental difference between Kawan and the claims of the PD is that Kawan always places the biometric reading device into the terminal, while the PD places the biometric device into the computing device (opener), original claims 3 and 17 of the PD. The most explicit discussions of Kawan, and all figures, including Fig. 7 of Kawan, always show that the smart card 66 only stores biometric information, while the biometric reader device is on the other side, namely in the terminal 68. It is much more inventive and novel, and more tamper proof with the biometric reader device being in the computing device as in claims 3 and 17. Applicant included the limitations of claims 3 and 17 into claims 2 and 16 and canceled claims 3 and 17. With these amendments claims 2 and 16, all by themselves, add patentable subject matter to their independent claims, since Kawan has nothing at all on using a biometrical reader device unconventionally.

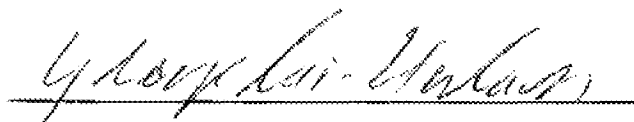
OA also stated that claim 20 is rejected under 35 U. S. C. 101 because a "carrier wave" is not patentable subject matter. Applicant would respectfully point out there are over 1000 issued patents since 2000, that have claims directed to a "carrier wave". Applicant would ask for reconsideration of the "101" rejection, or OA indeed means to state that are over 1000 recently issued US patents have invalid claims?

CLOSING STATEMENTS

Applicant respectfully submits that the claims as now put forward are patentable. Applicant points out that although amendments were made, overall no new limitations were introduced. Only already expressed limitations were combined into fewer claims. Furthermore, independent claims 4 and 20 already contains all unique limitations and were not amended. Applicant would respectfully contend, that if examiner undertakes a new search this was not necessitated by applicant's amendments. The OA already considered all limitations presented in the amended claim set, and applicant rearrangement of the existing limitations in itself does not require carrying out a new search. Thus, if a next OA would reject claims based on newly searched prior art, this next OA appropriately should not be made final. (This, of course, is only a hypothetical, since applicant is confident that in any case there exists no anticipatory prior art.)

Applicant further submits that this application is now in condition for allowance, which action is respectfully requested.

Respectfully,



George Sai-Halasz, PhD
Registration # 45,430

303 Taber Avenue
Providence, RI 02906

T: 401-427-0853, Fax 401-427-0319
E-MAIL - patents@computer.org

Cust. No.: **24299**